REMARKS

Reconsideration of the instant application is respectfully requested. The present amendment is responsive to the Office Action of December 21, 2004, in which claims 1-21 are presently pending. With regard to the art of record, each of claims 1-21 presently stands rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent Publication 2002/0144108 to Benantar. Claims 5-6, 12-13 and 19-20 are additionally rejected under 35 U.S.C. §103(a) as being unpatentable over Benantar. For the following reasons, however, it is respectfully submitted that the application is now in condition for allowance.

Each of the independent claims 1, 8 and 15 has been amended to include the language "wherein said proof of possession confirmation is constructed in a manner so as to prevent replay attacks by an impostor." Support for this amendment is found at least at page 6, line 7, through page 7, line 23 of the specification.

In contrast, paragraph [0085] of the Benantar '108 publication discusses "encrypted authentication data." However, this differs from a proof of possession confirmation in that the data (1) originates with the requesting subject; and (2) poses a target for cryptanalysis by adversaries which would reveal, if successful, the credentials by which the originating user may access the system. On the other hand, the corresponding information in the proof of possession confirmation as provided for in present claims is not incorporated in the certificate. As such, the proof of possession confirmation, as now claimed, is configured to prevent a replay attack. This capability is not taught or suggested by Benantar '108. Accordingly, it is respectfully submitted that each of the §102 and §103 rejections to the claims has been overcome.

In addition, claims 22-24 have been added with respect to the independent claims, and provide that the "sealed proof of possession is verifiable for compatibility with at

least one other of said plurality of data fields of said certificate request." Support for this amendment is found at least at page 8, line 23, through page 9, line 10 of the specification.

The Benantar '108 publication fails to teach that the subject public key is included within the encrypted package (as opposed to in the clear of a public key certificate request. Accordingly, through the additional claim language of claims 22-24, the term "sealed proof of possession" becomes more particularly defined with respect to the Benantar '108 publication and, as such, are separately patentable on this basis.

For the above stated reasons, it is respectfully submitted that the present application is now in condition for allowance. No new matter has been entered and no additional fees are believed to be required. However, if any fees are due with respect to this Amendment, please charge them to Deposit Account No. 09-0458 maintained by Applicant's attorneys.

Respectfully submitted,
THOMAS L. GINDIN, ET AL.

CANTOR COLBURN LLP
Applicants' Attorneys

By _____
Sean F. Sullivan
Registration No. 38,328
Customer No. 46429

Date: March 15, 2005
Address: 55 Griffin Road South, Bloomfield, CT 06002
Telephone: (860) 286-2929